CyberOps Associates v1.0 - Skills Assessment (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Introduction

You have been hired as a junior security analyst. As part of your training, you were tasked to determine any malicious activity associated with the Pushdo trojan.

You will have access to the internet to learn more about the events. You can use websites, such as VirusTotal, to upload and verify threat existence.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

- Evaluate event alerts using Squil and Kibana.
- Use Google search as a tool to obtain intelligence on a potential exploit.
- Use VirusTotal to upload and verify threat existence.

Content for this assessment was obtained from http://www.malware-traffic-analysis.net/ and is used with permission. We are grateful for the use of this material.

Required Resources

- Host computer with at least 8GB of RAM and 45GB of free disk space
- Latest version of Oracle VirtualBox
- Security Onion virtual machine requires 4GB of RAM using 25GB disk space
- Internet access

Instructions

You will find this assessment activity to be more “open-ended” than some of the activities that the student has experienced in this course. You may modify the amount guidance to optimize the learning experience for your students.

Part 1: Gather the Basic Information

In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

Step 1: Verify the status of services

a. Log into Security Onion VM using with the username **analyst** and password **cyberops**.

b. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.

c. When the nsm service is ready, log into Sguil or Kibana with the username **analyst** and password **cyberops**.

Step 2: Gather basic information.

a. Identify time frame of the Pushdo trojan attack, including the date and approximate time.

Events occur on 2017-6-27 from 13:38 to 13:44.

b. List the alerts noted during this time frame associated with the trojan.

ET POLICY PE EXE or DLL Windows file download HTTP

ET TROJAN Pushdo.S CnC response

ET CURRENT_EVENTS WinHttpRequest Downloading EXE

ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)

ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile

ET POLICY TLS possible TOR SSL traffic

ET TROJAN Backdoor.Win32.Pushdo.s Checkin

c. List the internal IP addresses and external IP addresses involved.

The internal IP address is 192.168.1.96, and the external IP addresses are 62.210.140.158, 119.28.70.207, 143.95.151.192,145.131.10.21, 208.67.222.222, 198.1.85.250, and 208.83.223.34.

Part 2: Learn about the Exploit

In this part, you will learn more about the exploit.

Step 1: Infected host

a. Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset? (**Hint**: NetworkMiner or internet search)

MAC address: 00:15:c5:de:c7:3b (Dell)

IP address: 192.168.1.96

b. Based on the alerts, when (date and time in UTC) and how was the PC infected? (**Hint**: Enter the command **date** in the terminal to determine the time zone for the displayed time)

The PC appears to be infected with a Pushdo malware on 27 June 2017 at 13:38 UTC.

How did the malware infect the PC? Use an internet search as necessary.

Pushdo is a trojan that is used to download and install malicious software. It can report back to control server IP address embedded in the code. The server listens on TCP port 80, like a web server.

Step 2: Examine the exploit.

a. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

matied.com/gerv.gun (119.28.70.207)

lounge-haarstudio.nl/oud/trow.exe (145.131.10.21)

vantagepointtechnologies.com/wp.exe (143.95.151.192)

Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?

gerv.gun	**0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272**
wp.exe	**79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48**
trow.exe	**94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1**

b. Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.

As of July 2020,

gerv.gun - 59/71 engines detected as a malicious Win32.exe file with a size of 236KB. It has other names, such as test and vector.tui. The target machine is one with Intel 386 or later processors and compatible processors. This executable file can scan for the hostname of the victim's computer, BIOS version and installation. It can also import suspicious APIs, touch files in the Windows directory, and access the Windows Registry. (https://www.hybrid-analysis.com/sample/0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272?environmentId=100**)**

wp.exe - 53/67 engines detected as a malicious Win32.exe file with a size of 300.5 KB. It has other names, such as test2, test_3. The target machine is one with Intel 386 or later processors and compatible processors. This malicious executable file is also related to the cerber ransomware. (https://www.hybrid-analysis.com/sample/79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48?environmentId=100**)**

trow.exe - 64/71 engines detected as a malicious Win32.exe file with a size of 323 KB. It has other names, such as Pedals, Pedals.exe, and test3. The target machine is one with Intel 386 or later processors and compatible processors. This file is used to contact www.tyms.com and www.sjbs.org.

c. Examine other alerts associated with the infected host during this timeframe and record your findings

The infected host 192.168.1.96 initiated a dns lookup for myip.opendns.com. The trojan reported back to the CnC at 27 June 2017 at 13:44 via encrypted traffic as indicated by TOR SSL traffic.

Step 3: Report Your Findings

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.

On 26 July 2017 at 13:38 UTC, the user at the computer with the IP address 192.168.1.96 was infected after visiting matied.com. In less than 10 minutes, three Windows executable files were downloaded, gerv.gun, wp.exe, and trow.exe from different domains:

matied.com/gerv.gun (119.28.70.207)

lounge-haarstudio.nl/oud/trow.exe (145.131.10.21)

vantagepointtechnologies.com/wp.exe (143.95.151.192)

The first two alerts from Sguil observed are attempting to connect to the IP address of matied.com website. The website matied.com and the downloaded file gerv.gun are considered as malicious according to VirusTotal. The victim computer had also downloaded the malicious files wp.exe and trow.exe.

The malicious files gerv.gun, trow.exe and the wp.exe can access Windows system files and gain information about the computer. A variant of a Pushdo trojan probably was downloaded by the user and the trow.exe is used to contact other domains, such as www.sjbs.org and www.tyms.com via encrypted traffic as indicated by TOR SSL traffic.